**DEPARTMENT OF HOMELAND SECURITY**

**[Docket No. USCBP-2020-0052]**

**Privacy Act of 1974; System of Records**

**AGENCY:** U.S. Customs and Border Protection, U.S. Department of Homeland Security.

**ACTION:** Notice of Modified Privacy Act System of Records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/U.S. Customs and Border Protection (CBP)-018 Customs Trade Partnership Against Terrorism System of Records." This system of records allows DHS/CBP to collect and maintain records about members of the trade community related to CBP's Customs Trade Partnership Against Terrorism (CTPAT) Program. Businesses accepted into the Program, called partners, agree to analyze, measure, monitor, report, and enhance their supply chains in exchange for greater security and facilitated processing offered by CBP. The CTPAT Program allows CBP to focus its resources on higher risk businesses and thereby assists the agency in achieving its mission to secure the border and facilitate the movement of legitimate international trade. CBP is reissuing this modified system of records notice alongside a Notice of Proposed Rulemaking, issued elsewhere in the Federal Register, to exempt this system of records from certain provisions of the Privacy Act.

**DATES:** Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**ADDRESSES:** You may submit comments, identified by docket number USCBP-2020-0052 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: James Holzer, Acting Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

*Instructions*: All submissions received must include the agency name and docket number USCBP-2020-0052. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

*Docket*: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

**FOR FURTHER INFORMATION CONTACT:** For general questions, please contact: Debra L. Danisek, CBP Privacy Officer, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Room 3.3D, Washington, D.C. 20229, or Privacy.CBP@cbp.dhs.gov or (202) 344-1610. For privacy questions, please contact: James Holzer, (202) 343-1717, Privacy@hq.dhs.gov, Acting Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

**SUPPLEMENTARY INFORMATION:**

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, the U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) proposes to modify and reissue a current DHS system of records titled, "DHS/CBP-018 Customs Trade Partnership Against Terrorism (CTPAT) System of Records."

DHS/CBP is reissuing this modified system of records notice to update its description of how CBP collects and maintains information pertaining to prospective,

ineligible, current, or former trade partners that participate in the CTPAT Program; other entities and individuals in their supply chains; and members of foreign governments' secure supply chain programs that have been recognized by CBP, through a mutual recognition arrangement or comparable arrangement, as being compatible with the CTPAT Program. DHS/CBP is updating this system of records notice to expand the category of records to include additional biographic data elements, and to clarify that CTPAT members may also submit information to DHS/CBP under the CTPAT Trade Compliance program, to include importer self-assessments and other documentation.

CBP uses the information collected and maintained through the CTPAT security and trade compliance programs to carry out its trade facilitation, law enforcement, and national security missions. In direct response to 9/11, CBP challenged the trade community to partner with the government to design a new approach to supply chain security—one that protects the United States from acts of terrorism by improving security while facilitating the flow of compliant cargo and conveyances. The result was the CTPAT Program—a voluntary government/private sector partnership program in which certain types of businesses agree to cooperate with CBP in the analysis, measurement, monitoring, reporting, and enhancement of their supply chains.

Businesses accepted into the CTPAT Program are called partners and agree to take actions to protect their supply chain, identify security gaps, and implement specific security measures and best practices in return for facilitated processing of their shipments by CBP. The Program focuses on improving security from the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination. The current security guidelines for CTPAT Program members address a broad range of topics including personnel, physical, and procedural security; access controls; education, training and awareness; manifest procedures; conveyance security; threat awareness; and

documentation processing. These guidelines offer a customized solution for the members, while providing a clear minimum standard that approved companies must meet.

Businesses eligible to fully participate in the CTPAT Program include U.S. importers and exporters; U.S./Canada highway carriers; U.S./Mexico highway carriers; rail and sea carriers; licensed U.S. Customs brokers; U.S. marine port authority/terminal operators; U.S. freight consolidators; ocean transportation intermediaries and non-operating common carriers; Mexican and Canadian manufacturers; and Mexican long-haul carriers.

CTPAT Program members in good standing may optionally participate in the CTPAT Trade Compliance program. Beginning in March 2020, the former Importer-Self Assessment (ISA) program was integrated into CTPAT as CTPAT Trade Compliance. DHS/CBP is updating this SORN to clarify the additional records collected as part of the CTPAT Trade Compliance program, which is limited to existing CTPAT members. To qualify for the CTPAT Trade Compliance program, an importer must submit an additional application via the CTPAT Portal and a) be a Member of the CTPAT Security Program and in good standing, b) meet the eligibility criteria laid out in the Eligibility Questions, and c) complete a Memorandum of Understanding (MOU) and Program Questionnaire.

To participate in the CTPAT Program, a company is required to submit a confidential, online application using the CTPAT Security Link Portal, https://ctpat.cbp.dhs.gov. The CTPAT Security Link Portal is the public-facing portion of the CTPAT system used by applicants to submit the information in their company and supply chain security profiles.

Additionally, the applicant business must complete a Supply Chain Security Profile (SCSP). The information provided in the SCSP is a narrative description of the procedures the applicant business uses to adhere to each CTPAT Security Criteria or

Guideline articulated for their particular business type (e.g., importer, customs broker, freight forwarder, air, sea, and land carriers, contract logistics providers) together with any supporting documentation. Data elements entered by the applicant business are accessible for update or revision through the CTPAT Security Link Portal. An applicant's SCSP must provide supply chain security procedures for each business in the applicant's supply chain, even if those businesses are not, or do not desire to become, partners of CTPAT separately. This information is focused on the security procedures of those businesses (e.g., whether the business conducts background investigations on employees), rather than the individuals related to those businesses (e.g., a list of employee names).

In addition to clarifying the inclusion of the CTPAT Trade Compliance program as part of the CTPAT System of Records, DHS/CBP is modifying Routine Use "E" and adding Routine Use "F" to conform to OMB Memorandum M-17-12. The previous Routine Use "F" has been re-lettered as Routine Use "H," the content of the previous Routine Use "G" has been modified to conform with current DHS guidance, and Routine Use "I" has been deleted. All subsequent Routine Uses have been renumbered to account for these changes. CBP is also expanding the category of records to assist in vetting individuals listed as associated with partner companies. The expanded categories of records include: date of birth (DOB); country of birth; country of citizenship; travel document number; immigration status information; driver's license information; Trusted Traveler membership type and number; and Registro Federal de Contribuventes (RFC) Persona Fisica (for Mexican Foreign Manufacturers, Highway Carriers, and Long Haul Carriers Only). Furthermore, DHS/CBP is expanding the collection of U.S. Social Security number beyond sole proprietors to now include the collection from all individuals listed as associated with partner companies. Additionally, this notice includes

non-substantive changes to simplify the formatting and text of the previously published notice.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-018 Customs-Trade Partnership Against Terrorism (CTPAT) system of records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/CBP may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, issued elsewhere in the Federal Register.

This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for

denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/CBP-018 CTPAT system of records. In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

**SYSTEM NAME AND NUMBER:** U.S. Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-018 Customs Trade Partnership Against Terrorism (CTPAT) System of Records.

**SECURITY CLASSIFICATION:** Unclassified, Sensitive Security Information, law enforcement sensitive.

**SYSTEM LOCATION:** Records are maintained at CBP Headquarters in Washington, D.C. and field offices, in the CTPAT Portal, and in a CBP collaborative intranet.

**SYSTEM MANAGER(S):** CTPAT Director, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Washington, D.C. 20229; (202) 344-3969. For CTPAT in general, contact Industry.Partnership@cbp.dhs.gov. For CTPAT Trade Compliance, contact ctpattradecompliance@cbp.dhs.gov.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** This system and program are authorized by 6 U.S.C. sec. 901 note (Security and Accountability for Every Port Act of 2006 (SAFE Port Act)), including 6 U.S.C. secs. 961-973. Pilot programs enhancing secure supply chain practices related to CTPAT are also authorized by Presidential Policy Directive/PPD-8, "National Preparedness" (March 30, 2011).

**PURPOSE(S) OF THE SYSTEM:** The purpose of this system is to verify the identity of CTPAT partners, determine enrollment level, and provide identifiable "low risk" entities with fewer random checks and facilitated processing. The information will be cross-referenced with data maintained in CBP's other cargo and enforcement databases and will be shared with other law enforcement systems, agencies or foreign entities, as

appropriate, when related to ongoing investigations or operations. Information will be used to analyze, measure, monitor, report, and enhance business supply chains to permit facilitated processing of CTPAT partner shipments by CBP.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Individuals, including Points of Contact, owners, and others associated with prospective, ineligible, current, or former CTPAT business entities; individuals associated with the supply chain of such CTPAT business entities; and individuals associated with business entities in foreign governments' secure supply chain programs that have been recognized by CBP, through harmonization, a mutual recognition arrangement (MRA), or comparable arrangement, as being compatible with the CTPAT Program.

**CATEGORIES OF RECORDS IN THE SYSTEM:** At the application level, information is collected from the applicant about itself and those members of its international supply chain. Pre-set fields of business-identifying information within the company profile portion of the online application include:

- Business Entity Type;
- Application Exception Token;
- Legal Business Name;
- Other Name(s) by which the Business is known (i.e., "Doing Business As"), if applicable;
- Business Telephone;
- Business Fax;
- Business Website Address;
- Business History;
- Physical Address(es);
- Mailing Address(es);
- Owner Type (e.g., Corporation\Partnership\Sole Proprietor);

- Years in Business;
- Number of Employees;
- Business Points of Contacts;
- First Name;
- Last Name;
- Date of Birth;
- Country of Birth;
- Country of Citizenship;
- Travel Document number (e.g., visa or passport number);
- Alien Registration Number
- Naturalization number;
- Driver's license information (e.g., state and country of issuance, number, date of issuance/expiration);
- Trusted Traveler membership type and number (e.g., FAST/NEXUS/SENTRI/Global Entry ID);
- Registro Federal de Contribuventes (RFC) Persona Fisica (needed for Mexican Foreign Manufacturers, Highway Carriers, and Long Haul Carriers Only);
- Title;
- Email Address (also used to log in to the Security Link Portal);
- Password;
- Telephone Number;
- Contact Type;
- U.S. Social Security numbers;
- Internal Revenue Service Business Identification Numbers;

- Customs assigned identification numbers (e.g., Importers of Record (IOR) number; Manufacturer Identification Numbers (MID) and Broker/Filer codes);
- Issue Papers, including information regarding whether the applicant is eligible for CTPAT membership or source record numbers for such information;
- Narrative description of supply chain security procedures for applicant and other entities in applicant's supply chain;
- Validation supporting documentation (e.g., bills of lading; audits—internal and external; proof of background checks; contractual obligations; via a letter from a senior business partner officer attesting to compliance; statements demonstrating compliance with CTPAT security criteria or an equivalent World Customs Organization accredited security program administered by a foreign customs authority; importer security questionnaire); and
- Account Status.

Information received from and confirmed to countries with which CBP has a Mutual Recognition Arrangement (MRA) includes:

- Legal Business Name;
- Other Name(s) by which the Business is known (i.e., "Doing Business As"), if applicable;
- Company Type;
- Date Partner Certified;
- Account Status;
- Vetting Status;
- Date Validation Completed;
- CBP Supply Chain Security Specialist (SCSS) Name;
- Office Assigned Name;
- Mutual Recognition Country;

- Business identifying numbers, e.g.:
    - Standard Carrier Alpha Code (SCAC);
    - IOR; and
    - MID.

By Applicant request, information received from, and forwarded to, foreign secure supply chain programs pursuant to a harmonization program may include:

- Legal Name;
- Doing Business As;
- Telephone Number;
- Fax Number;
- Web site;
- Owner Type;
- Business Start Date;
- Number of Employees;
- Brief Company History;
- Primary Address (Type, Name, Country, Street Address, City, State/Province, Zip/Postal Code);
- Mailing Address (Type, Name, Country, Street Address, City, State/Province, Zip/Postal Code);
- Primary Contact:
    - Email Address;
    - Type;
    - Salutation;
    - First Name;
    - Last Name;
    - Date of Birth;

    - Title; and
    - Telephone Number.
- Partner Notifications;
- Number of Entries;
- U.S. Department of Transportation (DOT) Issued Number;
- U.S. National Motor Freight Traffic Association Issued;
- SCAC;
- Dun & Bradstreet Number;
- Services Offered;
- Driver Sources;
- Entries related to harmonization country;
- Account Status;
- Vetting Status;
- Minimum Security Requirements/Security Profile Status;
- Validation Status; and
- Harmonization Status.

The CTPAT Security Profile includes:

- Account Number;
- Risking Status;
- Minimum Security Requirements (MSR) Status;
- Validation Type;
- Validation Closed Date;
- Validation Status;
- Validation Type Verification (Government Contact);
- Verification Type Start Date;

- Verification Type: (phone, visit, mutual recognition);
- Verification Visit address;
- Business Type; and
- Harmonization Host Program.

The records pertaining to the Trade Compliance Application Process:

- Trade Compliance Questionnaire:
    - Company name;
    - Business address;
    - Phone number;
    - Company Website;
    - Company type—public or private;
    - Company contact: name, date of birth, title, phone number and email address; and
    - Responses pertaining to Forced Labor.
- Memorandum of Understanding; and
- Annual Notification Letter (ANL);
    - Company Information: Organizational and/or Personnel Changes;
    - Import Activity Change records;
    - Internal Control Adjustments and Change records;
    - Risk Assessment Results;
    - Periodic Testing Results; and
    - Prior Disclosures.

**RECORD SOURCE CATEGORIES:** Records are obtained from the CTPAT applicant business; from CBP systems, including TECS, the Automated Targeting System (ATS), the Automated Commercial Environment (ACE); and from public sources. Information is also collected by the SCSS from the CTPAT applicant and other businesses during the

course of validating the business's supply chain and from foreign governments and multilateral governmental organizations with which CBP has entered into MRAs or other arrangements. To the extent a CTPAT partner applies for the CTPAT Trade Compliance program, CBP regulatory audit personnel collect information from the applicant as part of the Application Review Meeting.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those disclosures generally permitted under 5 U.S.C. 5 sec. 52a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agencies conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the federal government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this

system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To appropriate foreign governmental agencies or multilateral governmental organizations pursuant to an arrangement between CBP and a foreign government or multilateral governmental organization regarding supply chain security.

J. To an appropriate federal, state, local, territorial, tribal, or foreign governmental agencies or multilateral governmental organizations or other appropriate authority or entity when necessary to vet a CTPAT applicant or validate a CTPAT partner.

K. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be relevant in countering the threat or potential threat.

L. To a federal, state, tribal, or local agency, or other appropriate entity or individual, or foreign governments, in order to provide relevant information related to intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

M. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or when the information is relevant and necessary to the protection of life or property.

N. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation.

O. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant to a requesting agency's decision concerning the hiring or

retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit.

P. To a federal, state, local, tribal, or foreign governmental agency or multilateral governmental organization for the purpose of consulting with that agency or entity: (1) to assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

Q. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital health interests of a data subject or other persons (e.g., to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk).

R. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** DHS/CBP stores records in this system of records electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Records may be retrieved by any of the information listed in the categories of records above.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** The following records retention schedule for CTPAT is pending approval by NARA: information stored in CTPAT will be retained for the period during which the application is pending decision by CBP and for the period of active membership of the business entity, plus 20 years after membership has ended in the Program. Where information regarding the possible ineligibility of an applicant for CTPAT membership is found, it will be retained in the CTPAT system for 20 years from the date of denial to assist with future vetting, or consistent with the applicable retention period for the system of records from which such information was derived, whichever is longer.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** DHS/CBP safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/CBP has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**RECORD ACCESS PROCEDURES:** The CTPAT Portal provides access to those applicants or partners who have submitted information in the portal. The CTPAT partner interface allows participants to access and change the information they have provided at any time by accessing their business identifying information and CTPAT profile through

secure login procedures. CTPAT partners access the CTPAT Portal via https://ctpat.cbp.dhs.gov.

CTPAT partners have the ability to communicate with their assigned SCSS if they believe CBP has acted upon inaccurate or erroneously provided information. If this method is unsuccessful and CTPAT facilitated processing is denied or removed, the entity may make written inquiry regarding such denial or removal. The applicant should provide as much identifying information as possible regarding the business, in order to identify the record at issue. CTPAT participants may provide CBP with additional information to ensure that the information maintained by CBP is accurate and complete. The submitter will receive a written response to each inquiry. If CTPAT partnership is suspended or removed, the business may appeal this decision to CBP HQ, to the attention of the Executive Director, Cargo and Conveyance Security, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Room 2.2A, Washington, D.C. 20229.

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/CBP will consider individual requests to determine whether information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and CBP Freedom of Information Act Officer, whose contact information can be found at http://www.dhs.gov/foia under “Contacts Information.” If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress

Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying his/her agreement for the first individual to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

**CONTESTING RECORD PROCEDURES:** For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

**NOTIFICATION PROCEDURES:** See "Record Access Procedures" above.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** No exemption shall be asserted with respect to information requested from and provided by the CTPAT Program applicant including company profile, supply chain information, and other information provided during the application and validation process. CBP will not assert any exemptions for an individual's application data and final membership determination in response to an access request from that individual. However, the Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement agency has sought particular records may affect ongoing law enforcement activities. As such, pursuant to 5 U.S.C. sec. 552a(j)(2), DHS will claim exemption from sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. sec. 552a(k)(2) as is necessary and appropriate to protect this information.

Pursuant to exemption 5 U.S.C. sec. 552a(j)(2) of the Privacy Act, all other CTPAT Program data, including information regarding the possible ineligibility of an applicant for CTPAT membership discovered during the vetting process and any resulting issue papers, are exempt from 5 U.S.C. secs. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), and (e)(8); (f); and (g). Pursuant to 5 U.S.C. sec. 552a(k)(2), information regarding the possible ineligibility of an applicant for CTPAT Program membership discovered during the vetting process and any resulting issue papers are exempt from 5 U.S.C. secs. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). In addition, to the extent a record contains information from other exempt systems of records, CBP will rely on the exemptions claimed for those systems.

**HISTORY:** 78 FR 15962 (March 13, 2013).

*****

James Holzer,
Acting Chief Privacy Officer,
U.S. Department of Homeland Security.
[FR Doc. 2021-05647 Filed: 3/19/2021 8:45 am; Publication Date: 3/22/2021]